面向安全的轮流中继选择方案 *

秦小刚，邹　羿，黄开枝

(国家数字交换系统工程技术研究中心，郑州　450002)

摘　要：针对多中继轮流中继系统被窃听的问题，提出面向安全的轮流中继选择方案。首先提出了遍历的最优中继选择方案，并推导得到了保密速率的理论值；之后为降低复杂度，分别从降低计算复杂度和信道估计开销的角度设计了两种两阶段的次优中继选择方案，先缩小中继选择范围再进行搜索。仿真结果表明K-最大主信道中继选择方案能够以较低的复杂度实现最优保密速率。

关键词：轮流中继；物理层安全；中继选择；保密速率

中图分类号：TN92　　doi: 10.3969/j.issn.1001-3695.2017.09.0881

Secure-oriented relay selection schemes in successive relaying systems

Qin Xiaogang, Zou Yi, Huang Kaizhi

(*China National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: To solve eavesdropping problem in multi-relay successive relaying systems, this paper proposed a security-oriented relay selection schemes. First, it proposed optimal relay selection (OPRS) scheme through general search and deduced theoretical secrecy rate. To lower complexity, two different two-stage relay selection schemes which proposed first narrows the scope of relays from aspects of decreasing computation complexity and CSI overhead, respectively. Simulation results show that K-MMRS scheme can achieve optimal secrecy rate with lower complexity.

Key Words: successive relaying; physical-layer security; relay selection; secrecy rate

0　引言

协作通信技术能够成倍提高无线通信网络的频谱效率，但是一些中继站点的半双工特性限制了频谱效率的进一步提升[1]。半双工的中继站点不能同时收发信号，导致一次信息传输需要至少两个独立的时隙，导致了频谱效率的损失。全双工中继需要复杂的硬件设计，并且其存在的自干扰如果没能进行适当的处理反而会严重影响系统性能[2]，因此在很多场景下并不适用。

为了克服中继节点的半双工限制，一些学者提出了轮流中继(successive relaying, SR)的概念，通过合理安排多个半双工的中继交替转发信号来模拟一个全双工节点，达到了中继同时收发信号的效果[1,3~7]。利用 SR 技术，源节点与目的节点之间能够实现连续通信，从而提高了通信系统的频谱效率。在 SR 通信过程中，源节点与其中一个中继节点同时发送的信号会在另一个中继节点处相互干扰，来自另一中继转发的信号被称为中继间干扰(inter-relay interference, IRI)。现有研究表明利用信号处理技术能够克服 IRI 的影响，有效提高通信容量。

SR 技术引入多个中继节点给通信安全带来了新的问题，潜在地扩大了保密信号的传播范围，增加了中继链路被窃听的风险。另一方面，多中继网络也为安全通信提供了有利的空域协作资源，基于无线信道特征的物理层安全传输技术能够利用中继的协作资源，构造合法链路的优势通信条件保障安全通信，成为近年来的研究热点。中继选择技术[8~14]利用少数节点，能够以较低的复杂度实现最优或次优的安全性能，取得了很多的研究进展。其中文献[8]讨论了多种传输策略的最佳中继选择方案，并比较了它们的截获概率和可达分集增益；文献[9]针对多用户场景提出三种最小化保密中断概率的最优中继用户组合选择标准；文献[10]考虑采用改变自身策略以适应窃听者的方法，根据不同信道信息情况分别提出了最优中继选择方案，并进行了保密中断概率的推导；而文献[11~13]在中继选择的同时引入人工噪声的思想，选择其他节点发送友好干扰。文献[11]首次提出在多中继网络中选择一个中继和一个友好干扰节点增强网络安全性的思路；文献[12]则将该方法拓展到双向中继网络中，并证明当中继节点随机分散时保密速率优于传统双向中继网络的结论；文献[13]将该方法进一步推广，选择信道最佳的中继被选择来转发信息，其他节点均作为友好干扰发送噪声。此外文献

基金项目：国家“863”计划资助项目（，2014AA01A701）；国家自然科学基金资助项目（61379006，61521003，61701538）

作者简介：秦小刚（1982-），男，河南新乡人，工程师，助理研究员，学士，主要研究为移动通信（15639750306@163.com）；邹羿（1991-），男，山东济南人，硕士研究生，主要研究方向为无线物理层安全、协作通信等；黄开枝（1973-），女，安徽滁州人，教授，博导，主要研究方向为移动通信网络与信息安全等.

[14,15]考虑到节点的自私性，引入博弈论模型进行中继和干扰节点的选择。多中继的 SR 系统也面临着中继选择的问题。文献[16]考虑了 SR 系统中存在非信任中继的问题，将 IRI 消除技术与中继选择技术结合，提出了快速中继选择方法以取得较低的保密中断概率。但是还未有研究提出利用中继选择技术解决多中继 SR 系统的外部窃听问题。

针对上述问题，本文提出了面向安全的轮流中继系统中继选择方案，分别是最优中继选择(optimal relay selection, OPRS)方案、K-最大主信道中继选择(K-max main channels relay selection，K-MMRS)方案、K-最大中继间干扰中继选择(K-max IRI relay selection,K-MIRS)方案方案。其中 OPRS 方案从最大化保密速率的角度出发通过一维搜索的方法获得最优保密性能，并推导得到了系统保密速率的理论值，但是当中继数量较多时，OPRS 方案的计算复杂度、信道估计开销过高。为降低中继选择方案的复杂度，分别从最大化主信道、最大化 IRI 的角度出发提出 K-MMRS 方案、K-MIRS 方案。上述两个方案均为两阶段的次优中继选择方案，其基本思想是首先缩小中继选择范围然后进行遍历搜索，其中 K-MIRS 方案的计算复杂度最低，K-MMRS 方案的信道估计开销最低。最后，对上述方案进行了仿真验证，结果表明 K-MMRS 方案能够以较低的计算复杂度和信道估计开销实现最佳安全性能。

1 系统模型

本文研究如图 1 所示的多中继网络模型，该模型包含一个合法源节点(Alice)、一个合法接收节点(Bob)、一个窃听者(Eve)，以及一组相互之间距离较近的 N 个中继节点 $R_n \in C(1 \le n \le N)$，其中中继节点均采用放大转发协议。假设除了 Alice 配备 Na 天线外，网络中其他节点均为单天线，并且所有节点均工作在半双工模式。Alice 与 Bob 之间不存在直达径，因此它们之间的通信只能通过中继节点来建立。

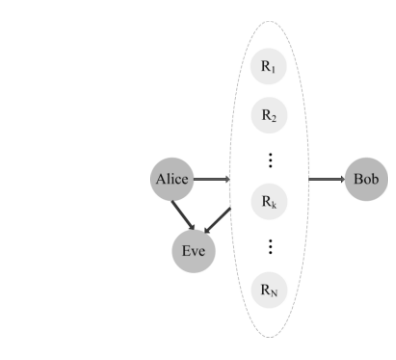


图 1 多中继网络模型

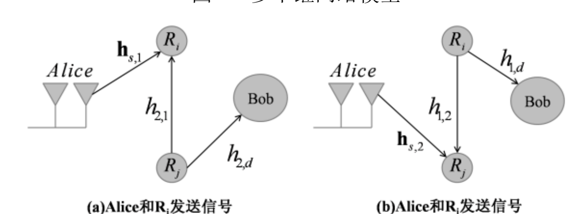


图 2 轮流中继系统通信过程示意图

假设在通信开始前 Alice 通过信道估计获取各节点之间的 CSI，并且基于一定的中继选择标准选择第 i 个中继(R_i)和第 j 个中继(R_j)参与通信，该假设与文献[13]及其参考文献相同。因此在通信过程中，只有被激活的中继参与通信，其他所有中继保持静默。SR 通信过程如图 2 所示。不失一般性，在奇数时隙，Alice 向 R_i 发送保密信息，R_j 转发前一时隙的接收信号；在偶数时隙，Alice 向 R_j 发送保密信息，R_i 转发前一时隙的接收信号。当中继之间的链路存在时，Alice 的发送信号与任意中继的发送信号会产生叠加，从而形成 IRI。IRI 的存在降低了合法节点的信道质量，会导致系统的保密速率为零。不失一般性，假设 Alice 向 R_i 发送信号 $\mathbf{s}(k)$，同时 R_j 向 Bob 转发前一时隙的接收信号 $y_j(k-1)$，其中 $\mathbf{s}(k)=\mathbf{W}(k)x(k)$，$\mathbf{W}(k)$ 和 $x(k)$ 分别为波束成形矢量和第 k 时隙的数据符号，并且 $E\left[\left|\mathbf{s}(k)\right|^2\right]=1$，此时中继和 Bob 的原始接收信号中包含 IRI。中继和 Bob 的原始接收信号如下所示：

$$y_i(k)=\sqrt{P_a}\mathbf{h}_{a,i}\mathbf{s}(k)+\sum_{p=1}^{k-1}\left(\sqrt{P_a}\mathbf{h}_{a,u}\mathbf{s}(p)+n_r(p)\right)\prod_{q=p}^{k-1}\sqrt{\alpha_v}h_{v,u}+n_r(k) \tag{1}$$

$$y_b(k)=h_{j,b}\sqrt{\alpha_j}y_j(k-1)+n_b(k) \tag{2}$$

其中：u、v 分别代表第 p 时隙和第 q 时隙发送信号的中继标号，当 $p=q=1$ 时，$\alpha_v=0$ 表示在第 1 时隙无中继参与信号转发。假设无线信道受到高斯白噪声的影响，$h_{i,j}$ 表示天线 i 到 j 之间的信道为非频率选择性瑞利分组衰落信道，该衰落服从均值为零、方差为 δ_{ij}^2 的复高斯分布，因此信道增益 $g_{ij}=\left|\delta_{ij}^2\right|$ 为指数分布；P_a 表示 Alice 平均功率限制，α_i 和 α_j 分别表示 R_i 和 R_j 在平均功率限制 P_r 下的放大系数，$n(k)$ 表示第 k 时隙的加性高斯白噪声变量。

采用文献[16]中 IRI 消除方案能够实现 IRI 在 Bob 处的完全消除，同时 Eve 由于信道差异无法进行类似的 IRI 消除，造成相邻保密信息之间的相互干扰，有效提高了 SR 系统的安全性。此外，Alice 采用迫零波束成形技术[7]使其信号在 Eve 处取得零陷。此时，在图 2 所示 SR 系统中进行 IRI 消除，中继、Bob 和 Eve 的接收信号分别可以表示为

$$y_i(k)=\sqrt{P_a}\mathbf{h}_{a,i}\mathbf{s}(k)+\sqrt{\alpha_j}h_{j,i}\sqrt{P_a}\mathbf{h}_{a,j}\mathbf{s}(k-1)+n_r(k) \tag{3}$$

$$y_b(k)=\sqrt{\alpha_j}h_{j,b}\sqrt{P_a}\mathbf{h}_{a,j}\mathbf{s}(k-1)+n_b(k) \tag{4}$$

$$y_e(k)=\sqrt{\alpha_j}h_{j,e}\sqrt{P_a}\mathbf{h}_{a,j}\mathbf{s}(k-1)+\sqrt{\alpha_j}h_{j,e}\sqrt{\alpha_i}h_{i,j}\sqrt{P_a}\mathbf{h}_{a,i}\mathbf{s}(k-2)+n_e(k) \tag{5}$$

其中：$\alpha_x=\dfrac{P_r}{\gamma_{a,x}+\gamma_{i,j}}$，$x\in(i,j)$，$\gamma_{i,j}=P_r g_{i,j}$。并且为了便于分析，假设来自 Alice 的信号和 IRI 都远远大于噪声部分，噪声的

影响被忽略。根据式(3)~(5)可得 Bob 和 Eve 两条链路的信干噪比(signal-to-interference-plus- noise ratio, SINR)：

$$\gamma_{B,j}=\frac{\gamma_{a,j}\gamma_{j,b}}{\left(\gamma_{a,j}+\gamma_{i,j}\right)\sigma^2} \tag{6}$$

$$\gamma_{B,i}=\frac{\gamma_{a,i}\gamma_{i,b}}{\left(\gamma_{a,i}+\gamma_{i,j}\right)\sigma^2} \tag{7}$$

$$\gamma_{E,j}=\frac{S}{N+I}\le\frac{S}{I}=\frac{\gamma_{a,j}}{\gamma_{i,j}\gamma_{a,i}}\left(\gamma_{a,i}+\gamma_{i,j}\right)=\gamma_{a,j}\left(\frac{1}{\gamma_{i,j}}+\frac{1}{\gamma_{a,i}}\right) \tag{8}$$

$$\gamma_{E,i}\le\gamma_{a,i}\left(\frac{1}{\gamma_{i,j}}+\frac{1}{\gamma_{a,j}}\right) \tag{9}$$

其中：$\gamma_{a,x}=P_a g_{a,x}$，$\gamma_{x,b}=P_r g_{x,b}$，$x\in(i,j)$。因此系统的保密速率为

$$R_s=\frac{1}{2}R_{s,i}+\frac{1}{2}R_{s,j} \tag{10}$$

其中：$R_{s,x}=\frac{1}{2}\left[\log_2\left(1+\gamma_{B,x}\right)-\log_2\left(1+\gamma_{E,x}\right)\right]^+$，$x\in(i,j)$。由于采用了 IRI 消除方案，可认为窃听信道容量小于主信道容量，此时 $R_{s,x}$ 中 $\log_2\left(1+\gamma_{B,x}\right)>\log_2\left(1+\gamma_{E,x}\right)$ 成立，因此：

$$R_s\approx 0.5\log_2\left(\frac{\left(1+\gamma_{b,i}\right)\left(1+\gamma_{b,j}\right)}{\left(1+\gamma_{e,i}\right)\left(1+\gamma_{e,j}\right)}\right) \tag{11}$$

当 SR 系统中存在 N 个可用的中继节点时，需要选择两个中继节点进行轮流转发以协助 Alice 与 Bob 之间的通信。基于上述分析建模，如何本文接下来将解决如何进行中继选择以保障通信安全的问题。

2 系统模型

与一般的中继系统不同，在 SR 系统中进行中继选择时需要考虑所选中继组合之间的信道对系统性能的影响。本章从 SR 系统安全性的角度出发，在进行中继选择时以系统保密速率为衡量指标，首先利用遍历的方法得到 OPRS 方案，并分析了中继数量较大时保密速率的理论值；为了降低中继选择的复杂度，从影响保密速率的不同角度出发提出了三种两阶段的中继选择方案，并分析对比了它们在计算复杂度分析、信道估计开销分析方面的表现。具体方案如下。

2.1 OPRS 方案

由于 R_s 表达式过于复杂，很难直接根据 R_s 的表达式选择最优的中继组合。为了得到最大的保密速率，最优的中继组合 R_i 和 R_j 的选择需要遍历所有可能的中继对，分别计算其保密速率，然后根据以下标准进行联合选择：

$$\left(i_{OS},j_{OS}\right)=\arg\max_{i,j\in C,i\ne j}R_s \tag{12}$$

下面推导当 SR 系统中可用的中继数量 N 较大时($N\to\infty$)系统保密速率的理论值。当中继数量较大时，最优中继到 Alice 之间的信道增益通常较大，可认为 $\gamma_{a,j}=\gamma_{a,i}=\max(\gamma_{a,n})$。由于 Alice 为多天线，此时 $\gamma_{a,n}$ 为 N 个相互独立、服从 $gamma\left(N_a,1/\lambda_{a,r}\right)$ 分布的随机变量，其中 $\lambda_{a,r}=\mathrm{P}_a\delta_{a,r}^2$。其累积分布函数 (Cumulative Distribution Function, CDF) 为 $F_X\left(x\right)=1-\frac{1}{\Gamma\left(N_a\right)}\Gamma\left(N_a,x/\lambda_{a,r}\right)$，由于 $\gamma_{a,j}=\gamma_{a,i}=\max\left(\gamma_{a,n}\right)$，因此 $\gamma_{a,i}$ 和 $\gamma_{a,j}$ 的 CDF 为

$$F_Y\left(y\right)=\left(1-\frac{1}{\Gamma\left(N_a\right)}\Gamma\left(N_a,y/\lambda_{a,r}\right)\right)^N \tag{13}$$

当 N 较大时可以认为 $\gamma_{a,j}=\gamma_{a,i}=EY$。由式可得

$$EY=\int_0^\infty ydF_Y\left(y\right)=yF_Y\left(y\right)\Big|_0^\infty-\int_0^\infty F_Y\left(y\right)dy \tag{14}$$

由于 $yF_Y\left(y\right)\Big|_0^\infty$ 和 $\int_0^\infty F_Y\left(y\right)dy$ 均无解，所以考虑将式(17)中的积分上限替换为 $NN_aP_a\delta_{a,r}^2$，即可解得 $EY\approx NN_aP_a\delta_{a,r}^2F_YNN_aP_a\delta_{a,r}^2-\int_0^{NN_aP_a\delta_{a,r}^2}F_Y\left(y\right)dy$。同理，可令 $\gamma_{j,b}=\gamma_{i,b}=EZ$，其中随机变量 $Z=\max\left(\gamma_{n,b}\right)$，$EZ$ 与 EY 的计算过程相似：

$$EZ\approx N\lambda_{r,b}F_Z\left(N\lambda_{r,b}\right)-\int_0^{N\lambda_{r,b}}F_Z\left(z\right)dz \tag{15}$$

其中：$\lambda_{r,b}=\frac{a}{a+\lambda_{r,r}}\mathrm{P}_r\delta_{r,b}^2$，$F_Z\left(z\right)=\left(1-\exp(-x/\lambda_{r,b})\right)^N$。

此时，整理 R_s 表达式可得

$$R_s\approx\left[\log_2\left(\frac{EY+\lambda_{r,r}+EYEZ}{EY+\lambda_{r,r}}\right)\left(\frac{\lambda_{r,r}}{2\lambda_{r,r}+EY}\right)\right] \tag{16}$$

由于中继数量较多，中继间信道增益的取值范围较广，可以通过最大化 R_s 的方法求解最优 $\lambda_{r,r}$，由式(19)可知，最大化 R_s 等价于最大化 $\left(\frac{EY+\lambda_{r,r}+EYEZ}{EY+\lambda_{r,r}}\right)\left(\frac{\lambda_{r,r}}{2\lambda_{r,r}+EY}\right)$，对该式求导并使导数为 0，即可得到最优 $\lambda_{r,r}$ 的取值：

$$\lambda_{r,r}=\left[\frac{-\left(EY\right)^2\pm\sqrt{\left(EY\right)^4-\left(EY-2EYEZ\right)\left(\left(EY\right)^3+\left(EY\right)^3EZ\right)}}{\left(EY-2EYEZ\right)}\right]^+ \tag{17}$$

为了衡量不同中继选择准则的性能，本文定义 f 为计算复杂度系数，$f=1$ 表示对应的中继选择算法需要遍历所有可能的中继对；定义 e 为需要交换的 CSI 开销系数，$e=1$ 时表示对应的中继选择算法需要获取全局信道状态信息。OPRS 方案采用一维搜索的方法来选择最优中继组合，因此需要计算所有可能的中继组合的 R_s，OPSRS 方案的 $f_{OP}=1$，共有 $C_N^2=\frac{N(N-1)}{2}$ 种。易得 OPRS 方案的时间复杂度为 $O(N^2)$，当 N 较大时，该

方案所需的计算时间将无法接受。采用 OPRS 方案时，所有中继链路、窃听链路和中继间的 CSI 需要估计，因此 $e_{OS}=1$，该方案下需要估计的 CSI 数量为 $1+3N+\frac{N(N-1)}{2}$。为了降低实现复杂度，本文在接下来的小节提出了三种快速中继选择方案，其基本思想是先通过一定的准则缩小候选中继的范围，再利用遍历方法确定参与通信的中继组合。

2.2　K-MMRS 方案

系统保密速率取决于主信道容量和窃听信道容量两方面，*K*-MMRS 方案从保证主信道容量的角度出发，首先选择 *K* 个包含最大主信道 $\gamma_n=\gamma_{a,n}\gamma_{n,b}$ 的中继以降低候选中继数量，然后再采用一维搜索的方法得到参与通信的中继组合：

$$\left(i_{MM},j_{MM}\right)=\arg\max_{i,j\in C_1,i\neq j}R_s \tag{18}$$

其中：C_1 表示 *K* 个 γ_n 最大的中继的集合。*K*-MMRS 方案采用了先减小中继选择范围再进行 R_s 计算与中继选择的方法，经过第一轮中继选择后可得到 K 个中继，因此第二轮需要计算的 R_s 的数量为 $\frac{K(K-1)}{2}$，$f_{MM}=\frac{K(K-1)}{N(N-1)}$。*K*-MMRS 方案在第一轮中继选择时需要获得所有 Alice 到中继、中继到 Bob 的信道，第二轮中继选择时需要获取 *K* 个中继间、中继与窃听者之间的信道，因此需要估计的 CSI 数量为 $1+2N+K+\frac{K(K-1)}{2}$，可得 $e_{MM}=\dfrac{1+2N+K+\frac{K(K-1)}{2}}{1+3N+\frac{N(N-1)}{2}}$。

2.3　K-MIRS 方案

SR 系统与一般半双工中继系统最大的不同在于 IRI 的存在，在本文考虑的 SR 通信系统中通过对 IRI 的处理，利用 IRI 恶化窃听条件，增大了主信道与窃听信道的差距，使 IRI 变为对系统安全有增益的因素。从最大程度恶化窃听信道的角度出发，提出 K-MIRS 方案。该方案首先在所有可能的中继组合中选择 K 个 IRI 最大(中继间信道增益最大)的中继组合，然后计算每个中继组合的并选择其中保密性能最好的中继对参与通信：

$$\left(i_{MI},j_{MI}\right)=\arg\max_{i,j\in C_2,i\neq j}R_s \tag{19}$$

其中：C_2 表示 IRI 最接近最优 $\lambda_{r,r}$ 的 K 对中继的集合。*K*-MIRS 方案也采用了两阶段中继选择的方法，但是与 *K*-MMRS 方案不同的是，其第一轮根据 IRI 筛选出的是 K 个中继组合，第二轮需要计算的 R_s 的数量为 K，因此 $f_{MI}=\frac{2K}{N(N-1)}$。在信道估计开销方面，*K*-OIRS 方案方案在选择 K 个中继组合时首先要获得所有中继之间的信道，然后第二阶段计算 R_s 时需要遍历 *K* 个中继对与其他节点(Alice、Bob、Eve)之间的信道，因此需要估计的 CSI 数量最多为 $1+\frac{N(N-1)}{2}+6K$，因此可得 $e_{MI}=\dfrac{1+\frac{N(N-1)}{2}+6K}{1+3N+\frac{N(N-1)}{2}}$。

3　仿真分析

为验证保密速率理论值以对比分析各中继选择方案的有效性，本文在 MATLAB 环境中对 SR 系统进行了相关的仿真分析。统一设置以下仿真参数：AWGN 的功率为 $\sigma^2=1$，Alice 到中继、中继到 Bob 的信道增益均值为 1，Alice 天线数为 4，发射功率 $P_a=P_r=30dBm$，蒙特卡洛仿真的次数为 10^4。

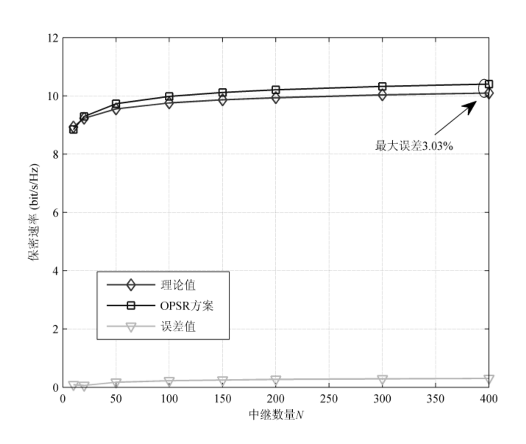


图 3　保密速率理论值与最优平均保密速率比较

中继数量变化时保密速率理论值与 OPSR 方案得到的最优保密速率变化情况如图 3 所示，其中假设中继间信道增益均值为 9。由图 3 可以看出，随着中继数量的增加，可达保密速率也增大，符合式(19)的规律，当 N 增大时，EY 和 EZ 的取值也增大，显然 R_s 是 EZ 的单调递增函数，当其他变量保持不变时，EZ 增大导致 R_s 的增加；而 R_s 不是 EY 的单调递增函数，其中 $\left(\frac{\lambda_{r,r}}{2\lambda_{r,r}+EY}\right)$ 部分甚至会随着 EY 的增长而降低，但是由于 $\lambda_{r,r}$ 的最优值会随着 EZ、EY 的变动而调整，弥补了 EY 变动带来的可能的损失。从物理意义理解，当可用中继的数量增加时，主信道容量取得较大值的可能性增加，受 IRI 的影响窃听信道容量保持较低水平，从而增大了保密速率的理论值。此外，由图 3 可知，随机信道下 OPSR 的平均保密速率略高于保密速率理论值，这与求解 EZ、EY 时缩小了积分上限有关，但是其与理论值的误差较小，在中继数量不超过 400 时最大误差仅为 3.03%。

图 4 展示了随着中继数量的增加，不同中继选择方案的平均保密速率变化情况，其中假设 $K=10$、中继间信道增益均值为 9。如图 4 所示，在相同的信道条件下，OPSR 方案能够得到最优的中继组合使得系统保密速率最大。*K*-MMRS 方案的性能次之，在中继数量较少时（$N<50$）几乎能取得与 OPSR 方案相同的保密速率，随着 N 的进一步增加，*K*-MMRS 方案与 OPSR 方案的差距逐渐增大，但是差距在可以接受的范围内，并且在

K=10 的条件下，计算复杂度、信道估计开销相比 OPSR 方案很小。计算复杂度和信道估计开销最低的 *K*-MIRS 方案在保密速率方面的性能最差，并且随着 N 的增加并没有改善，主要与其中继选择的标准有关，充分证实了 IRI 不是越大越好，在某个确定信道下存在最优值使得保密速率最大。

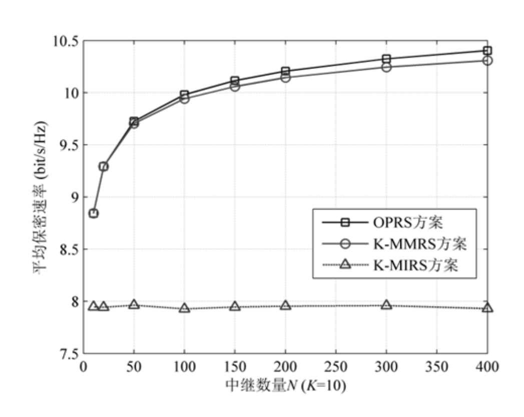


图 4　各中继选择方案的平均保密速率随中继数量变化情况

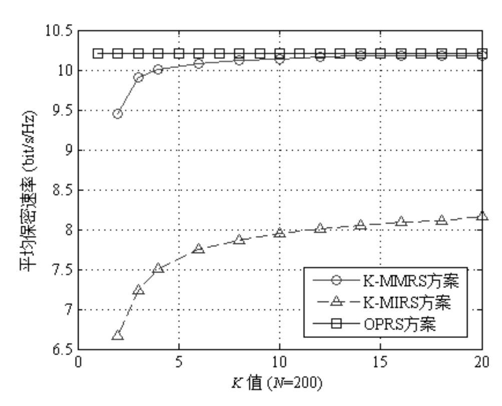


图 5　各中继选择方案的平均保密速率随 K 值变化情况

当 *K* 值变化时，各中继选择方案的平均保密速率变化情况如图 5 所示，其中假设 $N = 200$ 、中继间信道增益均值为 9。可以看出，各中继选择方案的平均保密速率都随着 *K* 值的增加而逐渐提高，*K* 值越大，各中继选择方案的计算复杂度、信道估计开销增加，以此为代价换取了更高的保密速率。此外，各中继选择方案的保密速率在 *K* 值较小时斜率较大，随着 *K* 值增大斜率变小，表明各中继选择方案会最终收敛。*K*-MMRS 方案在 $K = 8$ 时已经非常接近最优值，此时再增加 *K* 值带来的保密速率增益很小，而方案的复杂度会较高；K-MIRS 方案在 $K = 10$ 以后增速放缓，但其保密速率与 OPRS 方案差距较大，在 $K < 20$ 的条件下差距在 2 bit/s/Hz 以上。

图 6 展示了中继数量增加时，*K*-MMRS 方案达到最优保密性能时的平均 K 值、计算复杂度系数和 CSI 开销系数。上图表明，随着中继数量的增加，*K*-MMRS 方案达到最优保密性能所需要的 *K* 值也逐渐增大并基本呈线性规律增加，当中继数量较多 400 时，取 *K*=10 基本能取得最优保密速率；从下图可以看出，*K*-MMRS 的计算复杂度和 CSI 开销相比 OPRS 方案也有了明显的降低，其中计算复杂度系数小于 1%，CSI 开销系数小于 10%，证明 *K*-MMRS 方案能够以降低的计算复杂度与信道开销实现最优的安全性能。此外，随着中继数量的增加，计算复杂度系数与 CSI 开销系数也逐渐降低。

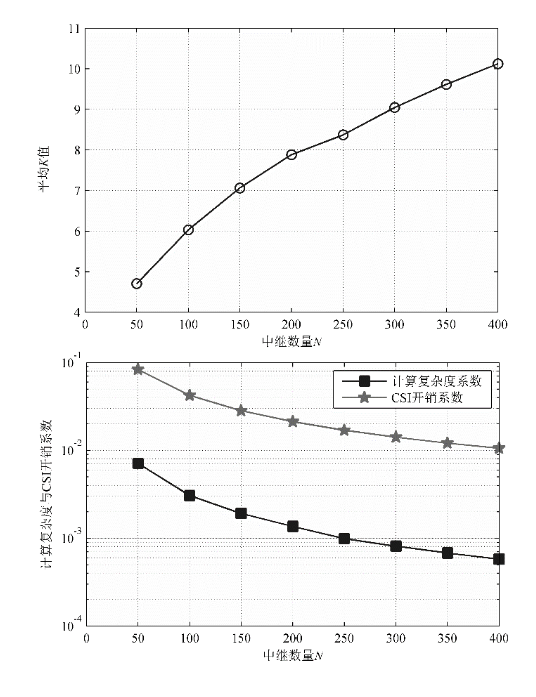


图 6　K-MMRS 方案性能分析

表 1 对比了本文提出的三种中继选择方案在保密速率、计算复杂度、信道估计开销方案的性能对比情况。其中在保密速率方面，OPRS 方案在任意场景下均为最优，在 K 相同时 K-MMRS 方案优于 K-MIRS 方案；在 N 和 K 相同时，三种方案根据计算复杂度性能排序（由低到高）：K-MIRS<K-MMRS<OPRS，K-MIRS 方案的计算复杂度最低；在 N 相同且较大时，三种方案根据信道估计开销性能排序（由低到高）为：K-MMRS<K-MIRS<OPRS，其中 K-MMRS 方案的信道估计开销最小。综上，OPRS 方案的保密性能最优但是中继数量较多时复杂度较高，K-MMRS 方案适用于信道变化较快的场景，而 K-MIRS 方案适用于对节点计算能力较低的场景。

表 1　各中继选择方案性能对比

性能 方案	保密 速率	计算 复杂度	信道 估计开销	适用场合
OPRS	最优	最高	最高	中继数量较少
K-MMRS	次优	一般	最低	信道变化较快
K-MIRS	最低	最低	一般	节点计算能力较低

4　结束语

本文针对 SR 系统中存在多个可用中继的场景，提出了多种面向安全的中继选择方案。首先，利用 IRI 消除方法提高了 Bob 的信号质量，使 IRI 只恶化 Eve 的信道，从而保障了 SR 系统的安全性。基于上述模型，提出通过遍历搜索的方法选取最优中继组合的 OPRS 方案，并推导了系统的保密速率理论值；针对 OPRS 复杂度和开销高的问题，进一步提出两种两阶段中

继选择方案。然后，从计算复杂度和信道估计开销方面分析、对比了不同中继选择方案的性能。仿真结果表明，OPRS 方案与所得保密速率理论值基本相同，最大化主信道容量的 K-MMRS 方案所取得的保密速率接近最优值。

参考文献：

[1] Yang S, Belfiore J C. Towards the optimal amplify-and-forward cooperative diversity scheme [J]. IEEE Trans on Information Theory, 2006, 53 (9): 3114-3126.

[2] Chen G, Yu G, Xiao P, et al. Physical layer network security in the full-duplex relay system [J]. IEEE Trans on Information Forensics & Security, 2015, 10 (3): 574-583.

[3] Rankov B, Wittneben A. Spectral efficient protocols for half-duplex fading relay channels [J]. IEEE Journal on Selected Areas in Communications, 2007, 25 (2): 379-389.

[4] Hu Y, Li K H, Teh K C. An efficient successive relaying protocol for multiple-relay cooperative networks [J]. IEEE Trans on Wireless Communications, 2012, 11 (5): 1892-1899.

[5] Xu P, Dai X, Ding Z, et al. Approaching MISO upper bound: design of new wireless cooperative transmission protocols [J]. IEEE Trans on Wireless Communications, 2011, 10 (8): 2725-2737.

[6] Nomikos N, Charalambous T, Krikidis I, et al. A buffer-aided successive opportunistic relay selection scheme with power adaptation and inter-relay interference cancellation for cooperative diversity systems [J]. IEEE Trans on Communications, 2015, 63 (5): 1623-1634.

[7] Kiim S H, Chaitanya T V K, Le-Ngoc T, et al. Rate maximization based power allocation and relay selection with IRI consideration for two-path AF relaying [J]. IEEE Trans on Wireless Communications, 2015, 14 (11): 6012-6027.

[8] Zou Y, Wang X, Shen W. Optimal relay selection for physical-layer security in cooperative wireless networks [J]. IEEE Journal on Selected Areas in Communications, 2013, 31 (10): 2099-2111.

[9] Fanl, Lei X, Duong T Q, et al. Secure multiuser communications in multiple amplify-and-forward relay networks [J]. IEEE Trans on Communications, 2014, 62 (9): 3299-3310.

[10] Yang L, Chen J, Jiang H, et al. Optimal relay selection for secure cooperative communications with an adaptive eavesdropper [J]. IEEE Trans on Wireless Communications, 2016, 16 (1): 26-42.

[11] Krikidis I, Thompson J S, Mclaughlin S. Relay selection for secure cooperative networks with jamming [J]. International Journal of Computer Science & Mobile Computing, 2009, 8 (10): 5003-5011.

[12] Chen J, Zhang R, Song L, et al. Joint Relay and Jammer Selection for Secure Two-Way Relay Networks [J]. IEEE Trans on Information Forensics & Security, 2012, 7 (1): 310-320.

[13] Wang C, Wang H M, Xia X G. Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks [J]. IEEE Trans on Wireless Communications, 2015, 14 (2): 589-605.

[14] Zhang N, Cheng N, Lu N, et al. Partner selection and incentive mechanism for physical layer security [J]. IEEE Trans on Wireless Communications, 2015, 14 (8): 4265-4276.

[15] 洪颖，黄开枝，罗文宇，等. 一种基于两次报价博弈机制的安全中继选择方法 [J]. 信息工程大学学报, 2014, 15 (5): 551-556.

[16] Wang W, Teh K C, Li K H. Relay selection for secure successive AF relaying networks with untrusted nodes [J]. IEEE Trans on Information Forensics & Security, 2016, 11 (11): 2466-2476.